|  |
| --- |
|   |
|  **政府組態基準****Microsoft IIS 10.0****TWGCB-04-014****(預告版V1.0)** |
|  |  |  |
|  |
| 國家資通安全研究院中華民國113年10月 |

**修訂歷史紀錄表**

|  |  |  |  |
| --- | --- | --- | --- |
| 項次 | 版次 | 修訂日期 | 說明 |
| 1 | 1.0 | 113/10/28 | 新編 |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
|  |

**目　次**

[1. 前言 1](#_Toc180701425)

[1.1 適用環境 1](#_Toc180701426)

[1.2 項數統計 1](#_Toc180701427)

[1.3 文件發行 1](#_Toc180701428)

[2. IIS政府組態基準列表 3](#_Toc180701429)

[3. 參考文獻 67](#_Toc180701430)

**表 目 次**

[表1 IIS設備組態基準項目統計 1](#_Toc180701431)

[表2 IIS政府組態基準列表 3](#_Toc180701432)

# 前言

政府組態基準(Government Configuration Baseline, 以下簡稱GCB)目的在於規範資通訊終端設備(如：個人電腦)的一致性安全設定(如：密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之疑慮。

## 適用環境

本文件適用於微軟Internet Information Services(以下簡稱IIS) 10.0版。

## 項數統計

政府組態基準針對電腦作業環境提供一致性安全基準與實作指引，供政府機關透過建立安全組態，提升資安防護能力。IIS 10.0組態基準共計53項設定項目，項目統計詳見表1。

1. IIS 10.0組態基準項目統計

|  |  |  |  |
| --- | --- | --- | --- |
| 項次 | 類別 | 項數 | 合計 |
| 1 | 基本設定 | 7 | 53 |
| 2 | 設定驗證與授權 | 5 |
| 3 | ASP.NET設定建議 | 12 |
| 4 | 要求篩選與其他限制模組 | 11 |
| 5 | IIS記錄 | 4 |
| 6 | FTP要求 | 2 |
| 7 | 傳輸加密 | 12 |
| 資安院整理 |

## 文件發行

本文件最新版本公布於國家資通安全研究院網站之「政府組態基準」專區，網址為<https://www.nics.nat.gov.tw/core_business/cybersecurity_defense/GCB/>。

# IIS 10.0政府組態基準列表

1. IIS 10.0政府組態基準列表

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定位置 | 設定路徑 | GCB設定值 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | TWGCB-04-014-0001 | 基本設定 | 網站內容存放位置 | * 這項原則設定決定網站內容存放之實體路徑位置是否可在系統磁區中
* 將網站內容存放在非系統磁區，可避免網站/應用程式耗盡系統磁碟空間，亦可避免網站/應用程式存在檔案讀取與寫入(File I/O)相關漏洞時，影響系統機密性或完整性
 | 站台 | IIS管理員\伺服器\站台\網站\動作\編輯站台\基本設定\編輯站台\實體路徑 | 存放在非系統磁區 |
| 2 | TWGCB-04-014-0002 | 基本設定 | 主機名稱 | * 這項原則設定決定是否每個站台都必須設定主機名稱
* 主機名稱也稱為主機標頭名稱(Host header)或網域名稱
* 每個Web網站可由「IP位址」、「連接埠」及「主機名稱」等3個要素構成一組唯一的識別，用來接收與回應請求
* 網站管理者可透過設定不同的「IP位址」、「連接埠」或「主機名稱」，達到在1台伺服器上架設多個網站之目的，所以，當「IP位址」與「連接埠」固定時，管理者就可運用不同之主機名稱以架設多個網站
* 所有站台都設定主機名稱，除便於識別外，可降低遭受DNS重新綁定攻擊之風險，以及防止透過IP掃描方式識別出IIS上所使用之應用程式
 | 站台 | IIS管理員\伺服器\站台\網站\動作\編輯站台\繫結\站台繫結\編輯\主機名稱 | 每個站台都必須設定主機名稱 |
| 3 | TWGCB-04-014-0003 | 基本設定 | 瀏覽目錄 | * 這項原則設定決定是否啟用瀏覽目錄功能
* 若啟用瀏覽目錄功能，當使用者沒有指定要瀏覽之檔案時，伺服器會依照預設文件之設定(例如：index.htm、default.htm或default.asp等)，將網頁傳送給使用者。若管理者停用預設文件之功能，或者伺服器找不到預設文件設定之檔案時，IIS會將該資料夾編製成目錄網頁，傳送給使用者，使用者藉此可得知網站目錄結構，所以如非必要，建議停用此功能
 | 伺服器 | IIS管理員\伺服器\IIS\瀏覽目錄\動作\開啟功能\動作\設為「停用」 | 停用 |
| 4 | TWGCB-04-014-0004 | 基本設定 | 應用程式集區識別 | * 這項原則設定決定所有應用程式集區之「識別」屬性內容
* 應用程式集區識別中所設定之帳號，是IIS實際執行工作者處理序「w3wp.exe」的帳號
* IIS內建ApplicationPoolIdentity帳戶，並賦予最小權限，供應用程式集區使用，可避免應用程式遭受威脅時，因執行帳號權限過高而造成系統更大危害，此外，亦可避免以往使用Network Service帳號執行時，因網站服務需求變更Network Service帳號權限後，導致其他同樣以Network Service帳號執行之應用程式獲得非必要的權限
* 預設應用程式集區(DefaultAppPool)以最小權限之ApplicationPoolIdentity身分執行。即使每個集區都設定ApplicationPoolIdentity做為識別，IIS會為不同集區建立不同之虛擬帳號做為對應，以達到應用程式集區獨立執行的效果
 | 應用程式集區 | IIS管理員\伺服器\應用程式集區\DefaultAppPool與其他自行新增的應用程式集區\動作\編輯應用程式集區\進階設定\處理序模型\識別 | ApplicationPoolIdentity |
| 5 | TWGCB-04-014-0005 | 基本設定 | 應用程式集區 | * 這項原則設定決定是否每個站台皆設定唯一之應用程式集區
* 每個站台設定唯一之應用程式集區，可集中運用資源以提升效能，並可避免因應用程式集區間之相互影響，而產生一個網站異常導致其他網站也異常之情況
* 所有站台預設皆使用DefaultAppPool應用程式集區
 | 應用程式集區 | IIS管理員\伺服器\站台\網站\動作\編輯站台\基本設定\應用程式集區\選取\應用程式集區 | 每個站台皆設定唯一的應用程式集區 |
| 6 | TWGCB-04-014-0006 | 基本設定 | 匿名使用者識別 | * 這項原則設定決定匿名使用者識別是否設為「應用程式集區識別」
* 將匿名驗證中之「匿名使用者識別」設定為「應用程式集區識別」，可確保匿名使用者以最小權限之身分執行，且可簡化站台管理工作
 | 伺服器 | IIS管理員\伺服器\IIS\驗證\動作\開啟功能\匿名驗證\動作\編輯\編輯匿名驗證認證\匿名使用者識別 | 應用程式集區識別 |
| 7 | TWGCB-04-014-0007 | 基本設定 | WebDAV功能 | * 這項原則設定決定是否停用WebDAV(Web Distributed Authoring and Versioning)功能
* WebDAV是一種以HTTP或HTTPS通訊協定為基礎，提供與遠端伺服器進行檔案維護之標準，允許用戶端在網頁伺服器上建立、移動及刪除檔案與資源
* 停用WebDAV以減少可能因存取控制設定錯誤而導致未經授權存取檔案之情況，進而提升網頁伺服器安全性
 | PowerShell | 開啟PowerShell視窗，執行下列指令：Remove-WindowsFeature Web-DAV-Publishing | 停用 |
| 8 | TWGCB-04-014-0008 | 設定驗證與授權 | 表單驗證需要SSL | * 這項原則設定決定使用表單驗證時，是否須以SSL方式進行資料傳輸
* 表單驗證會將使用者帳號與密碼以純文字格式傳送到伺服器，將可能導致使用者登入帳密資訊外洩，改採SSL連線方式保護登入資訊，有助於減少使用者資訊遭竊取之風險
 | 伺服器 | IIS管理員\伺服器\IIS\驗證\動作\開啟功能\表單驗證\動作\編輯\編輯表單驗證設定\Cookie設定\勾選「需要SSL」 | 需要SSL |
| 9 | TWGCB-04-014-0009 | 設定驗證與授權 | 表單驗證Cookie模式 | * 這項原則設定決定表單驗證是否使用Cookie
* 表單驗證Cookie模式選項如下：
1. 不使用Cookie：不使用Cookie
2. 使用Cookie：不論裝置為何，永遠使用Cookie
3. 自動偵測：如果裝置設定檔支援Cookie，則使用Cookie。否則，不使用Cookie。針對已知支援Cookie之桌面瀏覽器，ASP.NET會進行檢查以判斷是否啟用Cookie
4. 使用裝置設定檔：如果裝置設定檔支援Cookie，則使用Cookie。否則，不使用Cookie。ASP.NET不會進行檢查來判斷是否要在支援Cookie之裝置上啟用Cookie
* 使用者通過身分驗證登入站台後，表單驗證會在Cookie中維護一份驗證資訊，讓已通過驗證的使用者不需要對每個要求都輸入帳號密碼，當Cookie過期或找不到有效之Cookie時，使用者將被重新導向至指定登入頁面
* 使用Cookie管理使用者連線狀態，可藉由防止ASP.NET將Session資訊透過URL傳送，以避免Session ID在代理伺服器紀錄檔或瀏覽歷程紀錄中被找到，降低Session遭竊取之風險
* 預設設定為「使用裝置設定檔」
 | 伺服器 | IIS管理員\伺服器\IIS\驗證\動作\開啟功能\表單驗證\動作\編輯\編輯表單驗證設定\Cookie設定\模式 | 使用Cookie |
| 10 | TWGCB-04-014-0010 | 設定驗證與授權 | 表單驗證Cookie保護模式 | * 這項原則設定決定表單驗證Cookie之保護模式
* 表單驗證Cookie的保護模式選項如下：
1. 加密及驗證：同時指定用來協助保護Cookie之資料驗證及加密。此選項是使用已設定之資料驗證演算法，如果可供使用且金鑰夠長(48位元組以上)，可使用3DES來進行加密
2. 無：針對僅使用Cookie來啟用個人化且安全性需求較弱的站台，指定同時停用加密及驗證。此設定雖耗用最少資源，但不建議使用
3. 加密：指定Cookie使用3DES或DES進行加密，但是不會在Cookie上執行資料驗證
4. 驗證：此設定會確認Cookie內容在轉送過程中是否未被變更
* 採用「加密及驗證」保護模式，可確保Cookie資料之機密性與完整性，可降低Session遭到竊取或偽冒攻擊之風險
* 預設設定為「加密及驗證」
 | 伺服器 | IIS管理員\伺服器\IIS\驗證\動作\開啟功能\表單驗證\動作\編輯\編輯表單驗證設定\Cookie設定\保護模式 | 加密及驗證 |
| 11 | TWGCB-04-014-0011 | 設定驗證與授權 | 基本驗證需要SSL | * 這項原則設定決定使用基本驗證時，是否須以SSL方式進行資料傳輸
* 使用基本驗證時，使用者輸入使用名稱與密碼後，密碼以Base64編碼並傳送至伺服器進行驗證，因未加密，容易遭攻擊者側錄取得帳密資料，故若要使用基本驗證，應搭配SSL進行加密傳輸
 | 站台 | * 首先確認啟用https：IIS管理員\伺服器\站台\網站\動作\編輯站台\繫結
* SSL設定：IIS管理員\伺服器\站台\網站\IIS\SSL設定\動作\開啟功能\勾選「需要SSL」
 | 需要SSL |
| 12 | TWGCB-04-014-0012 | 設定驗證與授權 | credentials元素 | * 這項原則設定決定<credentials>元素是否可存在於設定檔(machine.config或web.config)中
* 使用表單驗證時，若使用<credentials>元素，會將帳密資訊儲存在設定檔，基於安全理由，建議從設定檔中移除<credentials>元素段落
 | 站台 | 開啟web.config與machine.config，檢視是否存在<credentials>元素段落 | 移除<credentials>元素段落 |
| 13 | TWGCB-04-014-0013 | ASP.NET設定建議 | 以retail模式部署Web應用程式 | * 這項原則設定決定是否以retail模式部署Web應用程式
* 以retail模式部署Web應用程式時，ASP.NET將停用追蹤輸出、停用偵錯功能，並停止將詳細系統錯誤訊息傳送給遠端使用者，以避免資訊洩漏
* 預設值為False
 | 系統檔案 | * 開啟machine.config檔案，路徑如下：%systemroot%\Microsoft.NET\Framework64或Framework\framework版本\CONFIG\machine.config
* 設定machine.config：在<system.web>下加入設定值<deployment retail="true" />
 | True |
| 14 | TWGCB-04-014-0014 | ASP.NET設定建議 | 偵錯功能 | * 這項原則設定決定是否啟用偵錯功能
* 開發人員通常在開發過程中啟用偵錯模式，網站上線後若未關閉偵錯模式，惡意人士將可利用此功能獲取應用程式相關資訊
* 雖然以retail模式部署Web應用程式時，即會停用偵錯功能，但基於縱深防禦概念，額外再個別停用偵錯功能，可降低因設定錯誤所造成之影響
* 設定為False，代表停用偵錯功能，設定為True，代表啟用偵錯功能
 | 伺服器 | IIS管理員\伺服器\ASP.NET\.NET編譯\動作\開啟功能\行為\偵錯 | False |
| 15 | TWGCB-04-014-0015 | ASP.NET設定建議 | 自訂錯誤訊息顯示模式 | * 這項原則設定決定當網頁發生錯誤時，以何種模式顯示自訂錯誤訊息頁面
* 自訂錯誤訊息顯示模式有3種：
1. 開啟(On)： 啟用自訂錯誤頁面。如果未指定預設的錯誤網頁時，則使用者與本機端都將顯示ASP.NET錯誤訊息頁面
2. 關閉(Off)： 停用自訂錯誤頁面，使用者與本機端都將顯示ASP.NET錯誤訊息頁面
3. 僅限遠端(RemoteOnly)：只對遠端使用者啟用自訂錯誤頁面，本機顯示ASP.NET錯誤訊息頁面
* 建議設定為開啟或僅限遠端，限制使用者僅能看到自訂錯誤頁面，以避免惡意人士利用此功能獲取應用程式相關資訊
* 預設值為僅限遠端(RemoteOnly)
 | 伺服器 | IIS管理員\伺服器\ASP.NET\.NET錯誤網頁\動作\開啟功能\動作\編輯功能設定\編輯錯誤網頁的設定\模式 | 開啟或僅限遠端 |
| 16 | TWGCB-04-014-0016 | ASP.NET設定建議 | HTTP詳細錯誤訊息顯示模式 | * 這項原則設定決定當網頁發生錯誤時，以何種模式顯示HTTP詳細錯誤訊息頁面
* HTTP詳細錯誤資訊可能包含有關應用程式如何運行之細節資訊，確保在遠端使用者端不顯示HTTP詳細錯誤資訊，可減少惡意人士獲取有關應用程式運作資訊之風險
* 藉由錯誤回應設定可決定HTTP詳細錯誤訊息頁面顯示方式：
1. 本機要求的詳細錯誤及遠端要求的自訂錯誤網頁(DetailedLocalOnly)：本機端顯示詳細錯誤訊息，非本機端顯示自訂錯誤頁面
2. 自訂錯誤網頁(Custom)：不管本機端或是遠端使用者，皆顯示自訂錯誤頁面
3. 詳細錯誤(Detailed)：本機端與遠端使用者皆顯示詳細錯誤訊息
* 預設值為DetailedLocalOnly
 | 站台 | IIS管理員\伺服器\站台\網站\IIS\錯誤網頁\動作\開啟功能\動作\編輯功能設定\編輯錯誤網頁的設定\錯誤回應 | 本機要求的詳細錯誤及遠端要求的自訂錯誤網頁或自訂錯誤網頁 |
| 17 | TWGCB-04-014-0017 | ASP.NET設定建議 | ASP.NET堆疊追蹤 | * 這項原則設定決定是否關閉網頁堆疊追蹤模式
* ASP.NET可透過設定<trace>元素來控制如何被蒐集、儲存及顯示追蹤結果。啟用追蹤後，每個網頁都會要求加入追蹤訊息，這些訊息會附加到頁面輸出或儲存在應用程式追蹤紀錄，建議停用追蹤，以減少惡意人士取得詳細追蹤資訊之風險
* 雖然以retail模式部署Web應用程式時，即會停用追蹤輸出，但基於縱深防禦概念，額外再設定停用追蹤功能，可降低因設定錯誤所造成之影響
 | 伺服器站台網頁 | * 伺服器級別設定：machine.config與web.config
* 站台級別設定：web.config
* 網站級別設定：每個ASP.NET網頁個別設定
 | 自設定檔與ASP.NET網頁中，移除所有Trace="true"或trace enabled="true"內容 |
| 18 | TWGCB-04-014-0018 | ASP.NET設定建議 | 工作階段狀態Cookie模式 | * 這項原則設定決定是否使用Cookie儲存工作階段狀態(Session state)
* 工作階段狀態Cookie模式選項如下：
1. 使用Cookie：不論瀏覽器或裝置是否支援Cookie，Cookie都會保存使用者資料
2. 使用URI：不論瀏覽器或裝置是否支援Cookie，呼叫的功能都會使用查詢字串儲存識別項
3. 使用裝置設定檔：ASP.NET根據HttpBrowserCapabilities設定決定是否使用Cookie。如果HttpBrowserCapabilities設定表示瀏覽器或裝置支援Cookie，就會使用Cookie，否則便會在查詢字串中使用識別項
4. 自動偵測：ASP.NET決定要求瀏覽器或裝置是否支援Cookie。如果要求的瀏覽器或裝置支援Cookie，AutoDetect便會使用Cookie保存使用者資料，否則便會在查詢字串中使用識別項。如果瀏覽器或裝置支援Cookie，但目前已停用Cookie，要求的功能還是會使用Cookie
* 使用Cookie管理使用者連線狀態，可藉由防止ASP.NET將Session資訊透過URL傳送，避免Session ID在代理伺服器記錄檔或瀏覽歷程紀錄中被找到，以降低Session遭竊取之風險
* 預設值為使用Cookie
 | 伺服器 | IIS管理員\伺服器\ASP.NET\工作階段狀態\動作\開啟功能\Cookie設定\模式 | 使用Cookie |
| 19 | TWGCB-04-014-0019 | ASP.NET設定建議 | httpOnlyCookies | * 這項原則設定決定Cookie是否只能經由HTTP(S)協定來存取，其餘之JavaScript、Silverlight或Flash等前端程式皆無法存取
* 設定網站中的Cookie屬性為HttpOnly，讓Cookie只供瀏覽器與網站伺服器間之網頁溝通，可避免Cookie被JavaScript等相關前端程式存取，以降低攻擊者利用網站既有的XSS漏洞並透過JavaScript取得Cookie資料之機會
 | 站台 | IIS管理員\伺服器\站台\網站\管理\設定編輯器\動作\開啟功能\區段\system.web\httpCookies\httpOnlyCookie | True |
| 20 | TWGCB-04-014-0020 | ASP.NET設定建議 | 電腦金鑰驗證方法(ASP.Net 3.5) | * 這項原則設定決定ASP.Net 3.5環境之電腦金鑰使用何種驗證方式
* 使用電腦金鑰，可設定加密及解密金鑰，用以協助保護表單驗證之Cookie資料與網頁層級的檢視狀態資料。電腦金鑰也可用來驗證跨處理序工作階段狀態識別
* 系統採用ASP.Net 3.5版本時，支援下列驗證方法：
1. AES(金鑰長度可為128, 192或256位元)
2. MD5
3. SHA1
4. TripleDES(金鑰長度為192位元)
* ASP.Net 3.5環境預設電腦金鑰驗證方法為SHA1
* 在變更.NET Framework版本設定中，分別有v2.0.x與v4.0.x兩種選項，「v2.0.x」表示.NET Framework版本包含3.0與3.5，則適用此項原則設定
* 確認版本方式：IIS管理員\伺服器\動作\變更.NET Framework版本，開啟確認版本
 | 伺服器 | IIS管理員\伺服器\ASP.NET\電腦金鑰\動作\開啟功能\驗證方法 | SHA1或AES |
| 21 | TWGCB-04-014-0021 | ASP.NET設定建議 | 電腦金鑰(ASP.Net 4.5) | * 這項原則設定決定ASP.Net 4.5環境之電腦金鑰使用何種驗證方式
* 使用電腦金鑰，可設定加密及解密金鑰，用以協助保護表單驗證之Cookie資料與網頁層級的檢視狀態資料。電腦金鑰也可用來驗證跨處理序工作階段狀態識別
* 系統採用ASP.Net 4.5版本時，支援下列驗證方法：
1. AES(金鑰長度可為128, 192或256位元)
2. MD5
3. SHA1
4. TripleDES(金鑰長度為192位元)
5. HMACSHA256
6. HMACSHA384
7. HMACSHA512
* ASP.Net 4.5環境預設電腦金鑰驗證方法為SHA1
* 在變更.NET Framework版本設定中，分別有v2.0.x與v4.0.x兩種選項，「v4.0.x」表示.NET Framework版本包含4.5，則適用此項原則設定
* 確認版本方式：IIS管理員\伺服器\動作\變更.NET Framework版本，開啟確認版本
 | 伺服器 | IIS管理員\伺服器\ASP.NET\電腦金鑰\動作\開啟功能\驗證方法 | HMACSHA256、HMACSHA384或HMACSHA512 |
| 22 | TWGCB-04-014-0022 | ASP.NET設定建議 | .NET信任層級 | * 這項原則設定決定是否指定套用到應用程式之程式碼存取安全性(Code Access Security, CAS)層級
* 可選擇之信任層級如下：
1. Full(internal)：指定未限制的權限。授予ASP.NET應用程式權限，以存取受制於作業系統安全性之任何資源。支援所有特殊權限操作。
2. High(web\_hightrust.config)：指定高程式碼存取安全性層級，ASP.NET應用程式預設無法執行下列任何一個動作：
	* 呼叫Unmanaged程式碼
	* 呼叫處理的元件
	* 寫入事件日誌
	* 存取「訊息佇列」服務佇列
	* 存取ODBC、OleDb或Oracle資料來源
3. Medium(web\_mediumtrust.config)：指定中程式碼存取安全性層級，表示除了高信任層級限制外，ASP.NET應用程式預設無法執行下列任何一個動作：
	* 在應用程式目錄外存取檔案
	* 存取登錄
	* 進行網路或網頁服務呼叫
4. Low(web\_lowtrust.config)：指定低程式碼存取安全性層級，表示除了中信任層級限制外，ASP.NET應用程式預設無法執行下列任何一個動作：
	* 寫入檔案系統
	* 呼叫Assert方法
5. Minimal(web\_minimaltrust.config)：指定最小的程式碼存取安全性層級，表示ASP.NET應用程式只具有執行權限
* 預設信任層級為Full(internal)
 | 伺服器 | IIS管理員\伺服器\ASP.NET\.NET信任層級\動作\開啟功能\信任層級 | Medium (web\_mediumtrust.config)、Low (web\_lowtrust.config)或Minimal (web\_minimaltrust.config) |
| 23 | TWGCB-04-014-0023 | ASP.NET設定建議 | X-Powered-By標頭 | * 這項原則設定決定是否移除X-Powered-By標頭
* X-Powered-By標頭為HTTP回應標頭，提供網頁伺服器在回應標頭中，呈現當前網頁應用程式所使用之技術
* 移除X-Powered-By標頭可避免攻擊者藉此取得網頁伺服器技術資訊(如使用ASP或PHP)，並利用特定版本已知漏洞對伺服器進行攻擊，以提升網頁伺服器安全性
 | 伺服器 | IIS管理員\伺服器\IIS\HTTP回應標頭\動作\開啟功能\X-Powered-By\動作\移除 | 移除 |
| 24 | TWGCB-04-014-0024 | ASP.NET設定建議 | 伺服器標頭 | * 這項原則設定決定是否移除伺服器標頭
* 伺服器標頭為HTTP回應標頭，呈現當前網頁應用程式所使用之技術
* 移除伺服器標頭是IIS 10的一項新功能，雖然透過回應標頭進行站台識別並非唯一方法，但移除後仍能增加難度，並阻止部分潛在攻擊者，從而有助於降低風險
 | 站台 | IIS管理員\伺服器\站台\網站\管理\設定編輯器\動作\開啟功能\區段\system.webServer\security\requestFiltering\removeServerHeader | True |
| 25 | TWGCB-04-014-0025 | 要求篩選與其他限制模組 | 允許的內容長度上限 | * 這項原則設定決定由用戶端傳送至伺服器之HTTP request之長度上限，以位元組為單位
* 當內容長度超過上限時，IIS將會記錄404.13狀態在日誌檔中
* 限制允許之內容長度，可避免大量之異常請求而導致網站服務異常，以維持網站可用性，亦可降低遭受緩衝區溢位攻擊之風險
* 預設值為30,000,000位元組，設為0代表長度無限制
 | 伺服器 | IIS管理員\伺服器\IIS\要求篩選\動作\開啟功能\動作\編輯功能設定\要求限制\允許的內容長度上限(位元組) | 30000000以下，但須大於0 |
| 26 | TWGCB-04-014-0026 | 要求篩選與其他限制模組 | URL長度上限 | * 這項原則設定決定URL字串(包含查詢字串)之長度上限，以位元組為單位
* 當URL長度超過上限時，IIS將會記錄404.14狀態在日誌檔中
* 限制可接受之URL最大長度，可避免因過長之URL導致伺服器異常
* 預設值為4,096位元組
 | 伺服器 | IIS管理員\伺服器\IIS\要求篩選\動作\開啟功能\動作\編輯功能設定\要求限制\URL長度上限(位元組) | 4096以下，但須大於0 |
| 27 | TWGCB-04-014-0027 | 要求篩選與其他限制模組 | 查詢字串上限 | * 這項原則設定決定查詢字串之長度上限，以位元組為單位
* 當查詢字串超過上限時，IIS將會記錄404.15狀態在日誌檔中
* 設定可接受的查詢字串長度，以避免因過長之查詢字串導致應用程式集區發生異常
* 預設值為2,048位元組
 | 伺服器 | IIS管理員\伺服器\IIS\要求篩選\動作\開啟功能\動作\編輯功能設定\要求限制\查詢字串上限(位元組) | 2048以下，但須大於0 |
| 28 | TWGCB-04-014-0028 | 要求篩選與其他限制模組 | 允許高位元字元 | * 這項原則設定決定查詢字串是否允許使用高位元字元(非ASCII字元)。高位元字元之範例包括：Ж、Ы或Я
* 當查詢字串因含有高位元字元而被拒絕時，IIS將會記錄404.12狀態在日誌檔中
* 禁止使用高位元字元，可確保URL中不會出現非ASCII文字，以避免發生輸入特殊字元或跳脫命令字元等攻擊語法
* 預設值為允許高位元字元
 | 伺服器 | IIS管理員\伺服器\IIS\要求篩選\動作\開啟功能\動作\編輯功能設定\一般\不勾選「允許高位元字元」 | 不允許 |
| 29 | TWGCB-04-014-0029 | 要求篩選與其他限制模組 | 允許雙重逸出 | * 這項原則設定決定是否允許URL雙重逸出，即是否允許URL請求使用雙重編碼技術
* 有些網站攻擊可以將URL請求利用雙重編碼技術(例如將”../”雙重編碼成為"%252E%252E%252F")，以繞過安全防護機制或造成應用程式非預期之反應
* 設定為不允許雙重逸出時，IIS會將URL請求利用正規化(Normalize)加以還原其原字元，並執行兩次，如第一次與第二次之結果不同，該請求就會被拒絕，並記錄404.11狀態在日誌檔中
* 預設值為允許高位元字元
 | 伺服器 | IIS管理員\伺服器\IIS\要求篩選\動作\開啟功能\動作\編輯功能設定\一般\不勾選「允許雙重逸出」 | 不允許 |
| 30 | TWGCB-04-014-0030 | 要求篩選與其他限制模組 | HTTP TRACE方法 | * 這項原則設定決定允許或拒絕使用HTTP TRACE方法
* HTTP TRACE方法會傳回用戶端提交的HTTP請求內容，攻擊者可利用此方法繞過HttpOnly限制，來存取HTTP標頭中所包含的機敏資訊(如驗證資料或Cookie)
* 預設值為允許
 | 伺服器 | IIS管理員\伺服器\IIS\要求篩選\動作\開啟功能\HTTP指令動詞\動作\拒絕指令動詞\輸入「TRACE」 | 拒絕 |
| 31 | TWGCB-04-014-0031 | 要求篩選與其他限制模組 | 允許未列出的副檔名 | * 這項原則設定決定是否允許未列出的副檔名在網頁伺服器上被執行
* 限制網頁伺服器只能執行特定之檔案類型，可提升安全性
* 在取消勾選「允許未列出的副檔名」後，必須將網站中所有使用到之副檔名(例如：.asax、.cs及.html等)與資料夾加入允許清單，網頁才能正常運作
 | 伺服器 | * 取消勾選：IIS管理員\伺服器\IIS\要求篩選\動作\開啟功能\動作\編輯功能設定\一般\不勾選「允許未列出的副檔名」
* 新增允許附檔名：IIS管理員\伺服器\IIS\要求篩選\動作\開啟功能\動作\允許副檔名
 | 不允許 |
| 32 | TWGCB-04-014-0032 | 要求篩選與其他限制模組 | 處理常式權限 | * 這項原則設定決定處理常式(Handler)可賦予之權限(包含無、讀取、寫入、指令碼及執行等5種選項)
* 設定處理常式不可同時具有「寫入」與「執行/指令碼」之權限，以降低在伺服器上執行惡意程式碼之風險
* 處理常式預設擁有「讀取」與「指令碼」權限
 | 伺服器 | IIS管理員\伺服器\IIS\處理常式對應\動作\開啟功能\動作\編輯功能權限 | 不能同時擁有執行/指令碼與寫入權限 |
| 33 | TWGCB-04-014-0033 | 要求篩選與其他限制模組 | 允許未指定的ISAPI模組 | * 這項原則設定決定是否允許未指定之ISAPI模組在此伺服器上執行
* 不允許未指定之ISAPI模組，可防止惡意使用者將未經授權之ISAPI二進制檔案複製到網頁伺服器中執行，以降低感染惡意程式之風險
 | 伺服器 | IIS管理員\伺服器\IIS\ISAPI及CGI限制\動作\開啟功能\編輯功能設定\不勾選「允許未指定的ISAPI模組」 | 不允許 |
| 34 | TWGCB-04-014-0034 | 要求篩選與其他限制模組 | 允許未指定的CGI模組 | * 這項原則設定決定是否允許未指定之CGI(.exe)程式在伺服器上執行
* 不允許未指定之CGI模組，可防止惡意使用者執行含有惡意指令碼的CGI程式，以降低感染惡意程式之風險
 | 伺服器 | IIS管理員\伺服器\IIS\ISAPI及CGI限制\動作\開啟功能\編輯功能設定\不勾選「允許未指定的CGI模組」 | 不允許 |
| 35 | TWGCB-04-014-0035 | 要求篩選與其他限制模組 | 動態IP限制 | * 這項原則設定決定是否藉由限制同一IP同時開啟連線數或限制同一IP在一段期間內發送之最大要求數量
* 透過動態IP限制功能，當超過限制時，IIS就暫時不處理來自該IP的請求，直接傳回HTTP錯誤以節省資源，不再耗費頻寬或CPU、記憶體處理要求，可降低DDoS攻擊影響
* 動態IP限制預設為停用
 | 伺服器 | IIS管理員\伺服器\IIS\IP位址及網域限制\動作\開啟功能\動作\編輯動態限制設定 | 啟用動態IP限制功能，並依需求設定「根據同時要求的數目拒絕IP位址」與「根據超過一段時間之要求數目拒絕IP位址」參數 |
| 36 | TWGCB-04-014-0036 | IIS記錄 | IIS記錄檔位置 | * 這項原則設定決定IIS記錄檔存放位置
* 記錄檔中含有IIS運作時之相關回應訊息，當網站服務異常或發生資安事件時，記錄檔可提供系統運作細節資訊供管理者參考。將記錄檔存放在受管制之非系統磁碟區中，將有助於降低發生系統磁碟區故障、惡意變更與刪除及遺失記錄之風險
* 預設存放位置為：%SystemDrive%\inetpub\logs\LogFiles
 | 伺服器 | IIS管理員\伺服器\IIS\記錄\動作\開啟功能\記錄檔\目錄 | 記錄檔存放至受管制的非系統磁碟區 |
| 37 | TWGCB-04-014-0037 | IIS記錄 | Advanced Logging | * 這項原則設定決定是否啟用Advanced Logging擴充模組
* Advanced Logging擴充模組提供豐富、彈性之資料集合與即時之記錄功能，可整合記錄檔，並允許管理者自訂記錄內容，或將不同之來源資料寫入記錄檔中，以備日後做為問題追踪之用
* 預設為啟用
 | 伺服器 | IIS管理員\伺服器\IIS\Advanced Logging\動作\開啟功能\動作\Enable Advanced Logging | 啟用 |
| 38 | TWGCB-04-014-0038 | IIS記錄 | 記錄檔格式 | * 這項原則設定決定記錄檔之格式
* 記錄檔的格式選項如下：
1. IIS：設定IIS使用Microsoft IIS記錄檔格式來記錄站台的相關資訊。此格式會由HTTP.sys處理，而且是「固定」的ASCII文字格式，這表示無法自訂要記錄的欄位。欄位會以逗號分隔，而時間使用本地時間記錄
2. NCSA：設定IIS使用「國家超級計算應用中心」(NCSA)通用記錄檔格式來記錄站台的相關資訊。此格式會由HTTP.sys處理，而且是「固定」的ASCII文字格式，這表示您無法自訂要記錄的欄位。欄位會以空格分隔，而時間會使用Coordinated Universal Time(UTC)位移記錄成本地時間
3. W3C：使用全球資訊網協會(W3C)擴充記錄檔格式來記錄站台的相關資訊。此格式會由HTTP.sys處理，而且是「可自訂」的ASCII文字格式，這表示可以指定要記錄的欄位。若要在「W3C記錄欄位」對話方塊中指定要記錄的欄位，請按一下「記錄」頁上的「選取欄位」。欄位會以空格分隔，而時間會使用Coordinated Universal Time (UTC)記錄
4. 自訂：設定IIS在自訂記錄模組使用自訂格式。選取此選項時，「記錄」頁面會停用，因為自訂記錄無法在IIS管理員中設定
* 記錄檔格式預設為W3C
 | 伺服器 | IIS管理員\伺服器\IIS\記錄\動作\開啟功能\記錄檔\格式 | W3C |
| 39 | TWGCB-04-014-0039 | IIS記錄 | 記錄事件目的地 | * 這項原則設定決定將網站訊息僅記錄在IIS記錄檔、或只寫入ETW(Event Tracing for Windows)事件記錄、或兩者都寫入
* 將網站訊息寫到Windows內之事件檢視器，管理者可使用標準查詢工具檢視即時記錄內容，亦可完整掌握整個網站之運作情形
 | 伺服器 | IIS管理員\伺服器\IIS\記錄\動作\開啟功能\記錄事件目的地 | 記錄檔和ETW事件二者 |
| 40 | TWGCB-04-014-0040 | FTP要求 | FTP SSL設定 | * 這項原則設定決定FTP是否使用SSL連線，以保護所有傳輸資料
* 選項如下：
1. 允許SSL連線：允許FTP伺服器支援與用戶端進行非SSL與SSL連線
2. 需要SSL連線：FTP伺服器與用戶端之間的通訊強制使用SSL加密
 | 伺服器 | IIS管理員\伺服器\FTP\FTP SSL設定\動作\開啟功能\SSL原則 | 需要SSL連線 |
| 41 | TWGCB-04-014-0041 | FTP要求 | FTP登入嘗試限制 | * 這項原則設定決定是否限制FTP帳戶登入失敗之最大次數
* 啟用FTP登入嘗試限制，可減輕攻擊者利用已發現之帳戶進行暴力攻擊所造成之影響
* 預設為停用
 | 伺服器 | IIS管理員\伺服器\FTP\FTP登入嘗試限制\動作\開啟功能\勾選「啟用FTP登入嘗試限制」 | 啟用 |
| 42 | TWGCB-04-014-0042 | 傳輸加密 | HSTS標頭 | * 這項原則設定決定是否在HTTP回應標頭設定使用HTTP嚴格傳輸安全(HTTP Strict Transport Security，以下簡稱HSTS)
* HSTS主要用來宣告瀏覽器與伺服器之間的通訊方式必須強制使用TLS/SSL加密通道，只要從伺服器端送出一個HSTS標頭(Header)給瀏覽器，就可以告訴瀏覽器在未來某段時間內一律使用SSL連接該網站(可設定包含所有子域名網站)，如果有發生憑證失效之情況，使用者將無法瀏覽該網站，如此一來便可大幅減少中間人攻擊之問題發生
 | 伺服器 | * IIS管理員\伺服器\IIS\HTTP回應標頭\動作\開啟功能\新增
* 名稱：Strict-Transport-Security
* 值：max-age=480(已使用HTTPS連線的網站480秒內不再檢查)
 | 名稱：Strict-Transport-Security值：max-age設為480以上 |
| 43 | TWGCB-04-014-0043 | 傳輸加密 | SSLv2 | * 這項原則設定決定是否停用SSLv2加密協定
* SSLv2存在已知弱點，為提升安全性應停用SSLv2加密協定
 | regedit | 執行以下步驟：1. 確認「HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server\Enabled」機碼是否存在，存在時，確認Enabled類型為DWord且資料欄位值為0，不存在時，請於SSL 2.0下新增機碼且命名為Server，並新增DWord值，名稱設為Enabled，資料欄位值設為0
2. 確認「HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server\DisabledByDefault」機碼是否存在，存在時，確認DisabledByDefault類型為DWord且資料欄位值為1，不存在時，請於SSL 2.0下新增機碼且命名為Server，並新增DWord值，名稱設為DisabledByDefault，資料欄位值設為1
3. 確認「HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client\Enabled」機碼是否存在，存在時，確認Enabled類型為DWord且資料欄位值為0，不存在時，請於SSL 2.0下新增機碼且命名為Client，並新增DWord值，名稱設為Enabled，資料欄位值設為0
4. 確認「HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client\DisabledByDefault」機碼是否存在，存在時，確認DisabledByDefault類型為DWord且資料欄位值為1，不存在時，請於SSL 2.0下新增機碼且命名為Client，並新增DWord值，名稱設為DisabledByDefault，資料欄位值設為1
 | 停用 |
| 44 | TWGCB-04-014-0044 | 傳輸加密 | SSLv3 | * 這項原則設定決定是否停用SSLv3加密協定
* 目前已知SSLv3存在POODLE弱點，為提升安全性應停用SSLv3加密協定
 | regedit | 執行以下步驟：1. 確認「HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server\Enabled」機碼是否存在，存在時，確認Enabled類型為DWord且資料欄位值為0，不存在時，請於SSL 3.0下新增機碼且命名為Server，並新增DWord值，名稱設為Enabled，資料欄位值設為0
2. 確認「HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server\DisabledByDefault」機碼是否存在，存在時，確認DisabledByDefault類型為DWord且資料欄位值為1，不存在時，請於SSL 3.0下新增機碼且命名為Server，並新增DWord值，名稱設為DisabledByDefault，資料欄位值設為1
3. 確認「HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client\Enabled」機碼是否存在，存在時，確認Enabled類型為DWord且資料欄位值為0，不存在時，於SSL 3.0下新增機碼且命名為Client，並新增Dword值命名為Enabled，最後資料欄位值設定為0
4. 確認「HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client\DisabledByDefault」機碼是否存在，存在時，確認DisabledByDefault類型為DWord且資料欄位值為1，不存在時，請於SSL 3.0下新增機碼且命名為Client，並新增DWord值，名稱設為DisabledByDefault，資料欄位值設為1
 | 停用 |
| 45 | TWGCB-04-014-0045 | 傳輸加密 | TLS 1.0 | * 這項原則設定決定是否停用TLS 1.0加密協定
* SSL加密協定與早期版本的TLS 1.0在2016年6月30日之後，已被視為不安全之加密協定
 | regedit | 執行以下步驟：1. 確認「HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server\Enabled」機碼是否存在，存在時，確認Enabled類型為DWord且資料欄位值為0，不存在時，請於TLS 1.0下新增機碼且命名為Server，並新增DWord值，名稱設為Enabled，資料欄位值設為0
2. 確認「HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server\DisabledByDefault」機碼是否存在，存在時，確認DisabledByDefault類型為DWord且資料欄位值為1，不存在時，請於TLS 1.0下新增機碼且命名為Server，並新增DWord值，名稱設為DisabledByDefault，資料欄位值設為1
3. 確認「HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client\Enabled」機碼是否存在，存在時，確認Enabled類型為DWord且資料欄位值為0，不存在時，請於TLS 1.0下新增機碼且命名為Client，並新增DWord值，名稱設為Enabled，資料欄位值設為0
4. 確認「HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client\DisabledByDefault」機碼是否存在，存在時，確認DisabledByDefault類型為DWord且資料欄位值為1，不存在時，請於TLS 1.0下新增機碼且命名為Client，並新增DWord值，名稱設為DisabledByDefault，資料欄位值設為1
 | 停用 |
| 46 | TWGCB-04-014-0046 | 傳輸加密 | TLS 1.1 | * 這項原則設定決定是否停用TLS 1.1加密協定
* TLS 1.1加密協定不支援較安全之新加密演算法，建議停用TLSv1.1以降低資訊洩露之風險
 | regedit | 執行以下步驟：1. 確認「HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server\Enabled」機碼是否存在，存在時，確認Enabled類型為DWord且資料欄位值為0，不存在時，請於TLS 1.1下新增機碼且命名為Server，並新增DWord值，名稱設為Enabled，資料欄位值設為0
2. 確認「HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server\DisabledByDefault」機碼是否存在，存在時，確認DisabledByDefault類型為DWord且資料欄位值為1，不存在時，請於TLS 1.1下新增機碼且命名為Server，並新增DWord值，名稱設為DisabledByDefault，資料欄位值設為1
3. 確認「HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client\Enabled」機碼是否存在，存在時，確認Enabled類型為DWord且資料欄位值為0，不存在時，請於TLS 1.1下新增機碼且命名為Client，並新增DWord值，名稱設為Enabled，資料欄位值設為0
4. 確認「HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client\DisabledByDefault」機碼是否存在，存在時，確認DisabledByDefault類型為DWord且資料欄位值為1，不存在時，請於TLS 1.1下新增機碼且命名為Client，並新增DWord值，名稱設為DisabledByDefault，資料欄位值設為1
 | 停用 |
| 47 | TWGCB-04-014-0047 | 傳輸加密 | TLS 1.2 | * 這項原則設定決定是否啟用TLS 1.2加密協定
* TLS 1.2為較新之加密協定，用以保護HTTP傳輸之機密性與完整性
 | regedit | 執行以下步驟：1. 確認「HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server\Enabled」機碼是否存在，存在時，確認Enabled類型為DWord且資料欄位值為1，不存在時，請於TLS 1.2下新增機碼且命名為Server，並新增DWord值，名稱設為Enabled，資料欄位值設為1
2. 確認「HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server\DisabledByDefault」機碼是否存在，存在時，確認DisabledByDefault類型為DWord且資料欄位值為0，不存在時，請於TLS 1.2下新增機碼且命名為Server，並新增DWord值，名稱設為DisabledByDefault，資料欄位值設為0
 | 啟用 |
| 48 | TWGCB-04-014-0048 | 傳輸加密 | NULL Cipher | * 這項原則設定決定是否停用NULL Cipher
* NULL Cipher無法確保資料機密性或完整性
 | regedit | * 確認下列機碼是否存在：

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL* 不存在時，表示停用
* 存在時，確認Enabled類型為DWord且資料欄位值為0
 | 停用 |
| 49 | TWGCB-04-014-0049 | 傳輸加密 | DES | * 這項原則設定決定是否停用DES加密套件
* DES已被視為安全性不足之加密套件
 | regedit | * 確認下列機碼是否存在：

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56* 不存在時，表示停用
* 存在時，確認Enabled類型為DWord且資料欄位值為0
 | 停用 |
| 50 | TWGCB-04-014-0050 | 傳輸加密 | RC4加密套件 | * 這項原則設定決定是否停用RC4加密套件
* 在TLS與SSL連線中使用RC4加密套件可能會讓攻擊者能夠進行中間人攻擊，並從加密之Session中還原純文字內容
 | regedit | * 確認以下4個機碼是否存在：
1. HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128
2. HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128
3. HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128
4. HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128
* 不存在時，表示停用
* 存在時，確認Enabled類型為DWord且資料欄位值為0
 | 停用 |
| 51 | TWGCB-04-014-0051 | 傳輸加密 | AES 128/128 | * 這項原則設定決定是否啟用AES 128/128加密套件
* AES 128/128已被視為安全性不足之加密套件
 | regedit | * 確認下列機碼是否存在：

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 128/128\Enabled* 不存在時，表示停用
* 存在時，確認Enabled類型為DWord且資料欄位值為0
 | 停用 |
| 52 | TWGCB-04-014-0052 | 傳輸加密 | AES 256/256 | * 這項原則設定決定是否啟用AES 256/256加密套件
* AES 256/256加密套件可用以保護HTTP傳輸之機密性與完整性
* 預設為啟用，且機碼值不存在
 | regedit | * 確認下列機碼是否存在：

HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256\Enabled* 不存在時，表示啟用
* 存在時，確認Server中Enabled類型為DWord且資料欄位值為0xFFFFFFFF
 | 啟用 |
| 53 | TWGCB-04-014-0053 | 傳輸加密 | TLS加密套件順序 | * 這項原則設定決定TLS加密套件順序
* 加密套件是一組命名組合，包含身分驗證、加密、訊息認證碼及金鑰交換算法，用於設定使用TLS協定之網路連線安全性。客戶端會依優先順序向伺服器發送其支援之加密套件清單，而伺服器則會從該清單中選擇一個加密套件進行回應
* 加密套件應從最強到最弱進行排序，以確保伺服器與用戶端之間使用較安全之加密傳輸
 | regedit | 針對「HKLM\System\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010002\Functions」機碼，其數值資料欄位設定如下：TLS\_AES\_256\_GCM\_SHA384,TLS\_AES\_128\_GCM\_SHA256,TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384,TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256,TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384,TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256,TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384,TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256,TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384,TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 | TLS\_AES\_256\_GCM\_SHA384,TLS\_AES\_128\_GCM\_SHA256,TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384,TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256,TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384,TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256,TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384,TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256,TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384,TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 |
| 資安院整理 |

# 參考文獻

1. Center for Internet Security。CIS Microsoft IIS 7 Benchmark v1.8.0

<https://www.cisecurity.org/cis-benchmarks/>

1. Center for Internet Security。CIS Microsoft IIS 8 Benchmark v1.5.1

<https://www.cisecurity.org/cis-benchmarks/>

1. Center for Internet Security。CIS Microsoft IIS 10 Benchmark v1.2.1

<https://www.cisecurity.org/cis-benchmarks/>